



Operations

85TH GROUP OPERATIONS SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>.

OPR: 85 GP/XP (MSgt Bradley K. Miles)
Supersedes 85 GPI 10-3, 1 April 1998

Certified by: 85 GP/CC (Col Phillip G. Gibbons)
Pages: 5
Distribution: F

This instruction implements JP 3-54, and AFI 10-1101, *Operations Security*. It prescribes procedures for conducting the 85th Group Operations Security (OPSEC) Program and applies to all staff agencies and units under the operational control of the Group. Send comments and suggested improvements to this instruction to on an AF Form 847, **Recommendation for Change of Publication**, through channels to 85 GP/XP.

SUMMARY OF REVISIONS

This supplement has been substantially revised and should be reviewed in its entirety.

1. OPSEC Policy. OPSEC is a command responsibility. Commanders and staff agency directors will ensure compliance with this Instruction and AFI 10-1101 as supplemented. Units will incorporate OPSEC into all aspects of exercise planning and participation.

2. Program Management. The Group OPSEC OPR is the 85 GP Deputy Commander (85 GP/CD).

2.1. The 85 GP OPSEC OPR will appoint a Group OPSEC Program Manager (PM).

2.1.1. Critical Information (CI) is best identified by individuals responsible for the development and execution of the operation. They possess the intimate familiarity necessary to properly apply the OPSEC process to the task at hand.

2.1.2. The PM should be assigned to either the operations or plans elements.

2.1.3. If OPSEC is assigned as an additional responsibility, it should be combined with other activities providing synergistic mission enhancement, like Plans or Tactical Deception.

2.1.4. In addition to the duties listed in AFI 10-1101, attachment 4, the PM will:

2.1.4.1. Develop and disseminate a commander approved (CI) list.

2.1.4.2. Ensure units and staff agencies comply with AFI 10-1101 as supplemented in this instruction.

2.1.4.3. Apply the OPSEC process during the deliberate planning phase of any operation or instruction.

2.1.4.4. Conduct an annual OPSEC program self-inspection, using the checklist in AFI 10-1101, attachment 5.

2.1.4.5. Conduct an annual review of this instruction and make changes as necessary.

2.1.4.6. Maintain contact with the NASKEF OPSEC PM and manage tenant OPSEC issues that could affect the 85 GP OPSEC program.

2.1.4.7. Ensure OPSEC POC information is widely publicized.

2.1.4.8. Provide assistance and guidance to unit PMs.

2.1.5. The Group OPSEC PM should be trained IAW AFI 10-1101 paragraph 3.2.4.

2.2. The following staff agencies and units will appoint an OPSEC Monitor:

2.2.1. 85 GP/CP

2.2.2. 85 OS

2.2.3. 85 MXS

2.2.4. 85 MSS (and Group Staff agencies, except for 85 GP/CP)

2.2.5. 85 SFS

2.2.6. 85 CES

2.2.7. 56 RQS

2.2.8. 932 ACS

2.3. Unit PMs should review all locally developed plans, orders, and directives to ensure adequate OPSEC considerations.

3. OPSEC Training. Each unit will develop and present training to newly assigned personnel within 30 days after arrival for duty. As a minimum, it should include:

3.1. OPSEC terminology and methodology.

3.2. Relationship of OPSEC to other security disciplines.

3.3. Use of shredders, STU-IIIs, and discretion in e-mail usage, personal contacts and conversations, to protect unclassified but sensitive, mission-related information.

3.4. Duty related mission critical information and OPSEC indicators.

3.5. Foreign intelligence threat to missions supported and conducted.

3.6. Individual responsibilities.

PHILLIP G. GIBBONS, COL
Commander, 85th Group

Attachment 1**85TH GROUP CRITICAL INFORMATION**

Origin of deployed forces
Destination of transient forces
Deployment/Redeployment timetables
Length of deployments
Personal information about deployed and permanent party personnel
Operation/exercise objectives
Exercise scenarios
Force strength (capabilities, limitations, effectiveness, expected uses, total numbers, level of training, and design information)
LIMFACS and shortfalls
Employment plans and tactics
- RAM implementation schedule
- Call sign changes
Employment targets and/or objectives for deployed and/or transient units
Introduction of new equipment/units
Command and Control Capabilities
Command Control, Communication Countermeasures capabilities
- Authentication Matrix
- Duress Words
- Sign/countersign
Electronic Attack and Electronic Protection capabilities
Command, control, communication, and computer information network configuration and critical node information
- Susceptibility of work center computers to unauthorized access through e-mail and internet usage
- Bulk encryption status
Reaction times and attainment times
Deception capability, use, or technique
Exercise or contingency plans that have any similarity or relationship to any current or recent real world situation or event
Limitations, reduced or recovery capability resulting from hostile actions

Position of equipment, supplies, or manpower in preparation for operations

- SRC/UCC stand-up

- Vehicle usage

VIP movement in anticipation of an exercise or contingency

Attack/air employment concepts

Personnel status reports (location, type, number)

- Strength reporting

- Augmentee usage

- Leave/TDY cancellations

Preparedness for NBC attacks

Stock levels of critical supplies (POL, MREs, Chem gear, munitions, etc.)

Aircraft Availability

- Number of aircraft

- Maintenance status

- Flight schedules

- Sea states

- Runway conditions